Safeguarding European Fundamental Rights or Creating a Patchwork of National Data Protection?

verfassungsblog.de/safeguarding-european-fundamental-rights-or-creating-a-patchwork-of-national-data-protection-2/

Christina Eckes , Vigjilenca Abazi Fr 9 Okt 2015

EU data protection law allows the transfer of personal data to countries outside the EU if the latter ensure '*adequate level of protection*' (Art. 25 of Directive 95/46). In the 2000 Safe Harbour Decision, the European Commission considered that the US provided such adequate level of protection through the 'Safe Harbour Privacy Principles', a scheme issued by the US Department of Commerce. Hence, personal information could be transferred from EU Member States to companies in the US that had signed up to these principles. On 6 October 2015, the Court declared the Commission's Safe Harbour Decision invalid because it disregards the significant limitations that US law imposes on privacy principles.

'Adequate' Is Not 'Identical', but 'Essentially Equivalent'

A key aspect in the Court's ruling is deciphering what constitutes an 'adequate' level of protection of personal data (paras 68 et seq of the judgment). The adequacy of the level of protection must be interpreted strictly due to firstly, the important role of the protection of personal data for the realisation of the fundamental right to private life and secondly, the large number of persons who may be affected by the transfer of personal data.

The Court concluded that EU law, while not providing a definition of what constitutes adequate protection, specifies that third countries must provide 'essentially equivalent' protection by 'domestic law' or 'international commitments'. The US Safe Harbour Principles fail to meet these criteria since they are adopted in an executive decision by the US Department of Commerce, which may be overridden by national security, public interest and law enforcement rules.

Protecting Fundamental Rights from 'Generalized' Invasion

Once the personal data has been transferred to the US, the National Security Agency (NSA) or the Federal Bureau of Investigation (FBI) can access it 'in the course of the indiscriminate surveillance and interception carried out by them on a large scale' (para 31). This is further complicated by the fact that oversight of intelligence agencies is carried out in secret and more often than not oversight bodies are poorly or belatedly informed. Considering the secrecy and lack of information flows in institutional oversight, it is perhaps not surprising that both the European Court of Justice and the Irish High Court relied explicitly on the revelations of Edward Snowden through 'leaked' documents.

The Court makes unequivocally clear that if public authorities have 'access on a generalised basis to the content of electronic communications [this] must be regarded as compromising the essence of the fundamental right to respect for private life as guaranteed by Article 7 [Charter of Fundamental Rights (CFR)]' (para 94). This conclusion is identical to the Court's ruling invalidating the Data Retention Directive, on which the Court heavily relies. Moreover, data protection rules, according to the Court, must ensure the possibility of the individual to access her personal data and have it rectified or erased. Anything else infringes 'the essence of the fundamental right to effective judicial protection' in Article 47 CFR and the rule of law (para 95). Indeed, as the Irish High Court asserted as well, the existing rules do not provide Union citizens an *effective* remedy.

In *Schrems*, just as in *Kadi,* the Court demonstrated that it is willing to go one step further and defend *EU standards of fundamental rights protection* in international relations. The sensitivity of international relations may also explain why the Court avoided examining the Safe Harbour Privacy Principles in substance. It instead invalidated the Commission's decision simply because it did not actually set out the state of 'domestic law' or 'international commitments' on data protection in the US (as required by Article 25(6) of Directive 95/46).

However, in the light of the US Supreme Court decision in Medellin, it remains highly questionable whether international commitments would be a sufficient safeguard against US authorities accessing data for reasons of national security or public interest.

Patchwork of National Data Protection?

On a first reading, *Schrems* gave considerable discretion to national supervisory authorities. The Court ruled that the Commission could not restrict the national supervisory authorities in carrying out their own assessment whether a third country complies with EU data protection law. National authorities have investigative powers, effective powers of intervention and the power to engage in legal proceedings. They may conclude whether a third country provides an adequate level of protection 'with complete independence' (para 57) and the Commission 'cannot eliminate or reduce' such powers of the national authorities (para 53). In this sense, the Court's decision opens the door to a complicated patchwork of national and even regional decisions of a multitude of data protection officers and their equivalents on whether or not data may be transferred to the individual company in the individual case.

Only five days earlier, the Court of Justice had ruled in Weltimmo that under certain circumstances, such as operating services in the native language and having representatives in a Member State, a company could be held accountable by that Member State's national data protection agency despite not being headquartered in the country. The combination of the two rulings seems to indicate that the Court prioritises effective decentralized data protection over uniformity. At the same time, the Court drew a uniform red line by declaring access on a generalized basis an infringement of fundamental rights. In their assessment, national supervisory authorities may not cross this line.

EU Data Protection Legislation and the TTIP Negotiations

The Court's ruling has immediate implications for the on-going process of adopting new EU data protection legislation, as well as the EU's position in the current negotiations of an umbrella agreement on data protection with the US. This is particularly interesting since the Court could have answered the preliminary questions without addressing the validity of the Commission's safe harbour decision. It could hence be accused of actively meddling with politics.

As the Court set out in considerable detail (paras 11 et seq), the Commission had already admitted problems with the safe harbour rules in 2013. Moreover in 2014, the European Parliament had specifically called for suspension of the safe harbor rules. Yet in practice they remained in place. While the European Parliament had no means to force suspension, the Civil Liberties Committee specifically reminded the negotiators that Parliament's consent to the final TTIP agreement could be endangered if data privacy rights were not adequately protected. It demanded a horizontal exception for EU data protection law. In fact, TTIP but also the Trade in Services Agreement (TiSA) are likely to exclude privacy and data protection entirely and leave the regulation to the new data protection umbrella agreement.

Schrems puts pressure on the Commission to speed up the negotiations with the US. This is also echoed by the private sector which points at the extra-costs resulting from legal uncertainty after the ruling. At the same time, *Schrems* does not only illustrate the differences in data protection in the EU and the US, but also lets the data protection rules drift further apart. This may ultimately result in an insurmountable obstacle for data exchange.

This article has previously been posted on the UK Constitutional Law Blog and is republished here with kind permission.

SUGGESTED CITATION Eckes, Christina; Abazi, Vigjilenca: *Safeguarding European Fundamental Rights or Creating a Patchwork of National Data Protection?, VerfBlog,* 2015/10/09, http://verfassungsblog.de/safeguarding-european-fundamental-rights-or-creating-a-patchwork-of-national-data-protection-2/.